UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,261	12/31/2003	Ryan Charles Catherman	RPS920030206US2	8466

45503 7590 09/17/2008
DILLON & YUDELL LLP
8911 N. CAPITAL OF TEXAS HWY.,
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
TURCHEN, JAMES R	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
09/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/749,261	**Applicant(s)** CATHERMAN ET AL.
	Examiner JAMES TURCHEN	**Art Unit** 2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 June 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8,10-15,17-22 and 24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,10-15,17-22 and 24* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

In view of the appeal brief filed on 06/23/2008, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139

Response to Arguments

Applicant's arguments filed 05/16/2008 have been fully considered but they are not persuasive. Examiner respectfully disagrees with applicant regarding the argument that Challener does not teach or suggest the specific criteria for performing the inserting of the endorsement certificate into the device, namely “only when said endorsement key is confirmed…" In paragraph 23 of Challener there is a public key P2 (the endorsement key) is sent over along with the certificate C1 (of the signing key pair). The CA checks the accuracy of the certificate, C1, and then makes a certificate, C2, for public key, P2. It is inherent in the paragraph, that if the certificate is not accurate or valid, then there will be no certificate made and sent to the device, therefore the device will not insert the certificate if there is no certificate. When the certificate is inserted into the device [*paragraph 24*], it is because the endorsement key was confirmed having been generated from within a valid device. Woods is analogous to the combination of Challener and Smith as Woods and Smith are both belonging to class 380. Paragraph 39 was cited as the addition of the temporary keys from figure 6 makes the system more secure. Paragraph 4 of Woods also states that asymmetric encryption makes the system much more secure because it is difficult to break an encryption unless the private key is known.

Applicant's arguments, see B.3, filed 05/16/2008, with respect to the rejection(s) of claim(s) 14-16 under 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Challener in view of Felt et al. (US 2002/0138735 hereafter Felt).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 8, 10-22, and 24 rejected under 35 U.S.C. 103(a) as being unpatentable over Challener in view of Smith (US 6,233,685) and in further view of Wood.

Regarding claim 1:

Challener discloses generating for a valid device an endorsement key pair that includes a private key and a public key (paragraphs 0022-0024, public key, P2, and private key, P4), wherein said private key is not public readable (inherent trait of public/private key pairs); creating a non-public, signing key pair (paragraph 0021 and 0024, endorsement key with public key, P1, and private key, P3) [Examiner interprets non-public key pair in light of the specification as a key pair that is used amongst a few select entities or only temporarily in the communication.] ; and inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device (paragraph 0024, certificate, C2) only when said endorsement key is confirmed having been generated from within a valid device (it is common in the art that the key is generated within the device (see US 6,973,191 for reference)).

Challener does not discloses wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined method selected from among expiration of a preset amount of device manufacturing time and manufacture of a preset number of devices from the plurality of valid devices, however, it is obvious that the key changes from device to device, thus changing after a preset amount of device manufacturing time. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the key pair to change from a single device to a plurality of devices as it would have yielded less overhead due to generation of less keys.

Challener does not disclose verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair (inherent property of identity based authentication of a CA to contain information about the key pair). Smith et al. discloses in columns 8 lines 35-67 to column 9 lines 1-28, verifying at a credential server (Certificate Authority, CA) a signature of said endorsement key (device key as used in Smith et al.) is a public signing key (authorities public key) of signing key pair. It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method of Challener for generating an endorsement key, creating a signing key, and inserting an endorsement certificate with the method of Smith et al. for verifying that a key is in fact a key from the device in order to certify the device (Smith et al, column 8 lines 60-63).

Challener and Smith do not teach wherein said signing key pair is a single use parameter, said method further comprising immediately destroying said signing key pair within said device following a creation of said endorsement key. Wood et al. discloses using a temporary key pair (figure 6, step 605-645; paragraphs 36-39) after which the key is no longer used (discarded). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method and system of claims 1 and 17 disclosed by Challener and Smith et al. with the temporary key of Wood et al. in order to provide additional security (Wood et al, paragraph 0039).

Claim 2:

Smith et al. discloses providing a signing key certificate for said signing key pair, said signing key certificate including a public singing key of said signing key pair; and forwarding said signing key certificate via a secure communication medium to said credential server (column 9 lines 12-17, the device presents the certificate and the information contained in it (it is inherent to include the public key of the certificate with the certificate) to the requesting party (CA)).

Claim 3:

Challener al. discloses signing said public key of the endorsement key pair (paragraph 0023, the public key, P2, and the certificate, C1, are sent to the CA (it is inherent to send information encrypted by the public key of the certificate along with the certificate)) with a public signing key (P1) of said signing key pair when creating the endorsement key (EK); and forwarding a resulting signed EK to said credential server to initiate a credential process (paragraph 0023).

Claim 4:

Challener discloses receiving said signed EK at said credential server (paragraph

0023); comparing the public signing key within the signing key certificate with a signature from the signed EK (it is inherent to use the public key of the certificate); and when the public signing key matches the signature, confirming (verifying) said EK as originating from a valid device (paragraph 0023).

Claim 5:

Challener discloses a CA which inherently stores the credential in a database of said credential server; monitors for a request from a customer to provide said certificate to said device (this is done with the request for certification); and following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device (this is done after the certification).

Claim 6:

It is inherent in TCPA for the endorsement key to be once writable, public readable (see TCPA Spec 1.1b, page 261) therefore it would have been obvious to one of ordinary skill in the art to make the certificate once writable, public readable.

Claim 8:

Smith et al. discloses that the CA can be a remotely located third party with a secure connection (column 8 lines 31-43).

Claims 10 and 11:

Challener discloses creating/manufacturing and authenticating a Trusted Platform Module in the Abstract and paragraph 6.

Claims 12 and 13:

Challener discloses a processor (Figure 1, 110), a TPM chip (111), a bus for interconnecting said processor and said TPM chip (it is inherent to connect two or more components through a bus), a network interface with communication means for connecting said TPM to a secure credential server (Communications Adapter 134 and Network 160). The means whereby said TPM is able to verify an endorsement key pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture of the TPM, means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed EK, and means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate as the system of the method claims 1-5, rejected under the same arguments.

Claims 17-22, 24, and 25 correspond to the system of method claims 1-6, 8, and 9. Claims 17-22, 24, and 25 are rejected under the same logic as claims 1-6, 8, and 9.

Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener in view of Felt.

Regarding claim 14:

Challener discloses a data processing system utilized for issuing endorsement certificates, comprising:

a processor (paragraph 23, it is inherent that a certificate authority (CA) has a processor);

a memory coupled to said processor via an interconnect (paragraph 23, it is inherent that a certificate authority has a memory coupled to a processor via a bus);

a security mechanism for ensuring optimum security of processes within said data processing system (paragraph 23, it is inherent that a certificate authority has at least one security mechanism);

input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices (paragraph 23, P1 is sent over the internet to CA; it is inherent that the CA is capable of receiving/sending); and

secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key (paragraphs 23 and 24, the bundle (containing a certificate, public key) is signed by the public signing key and decrypted with the private signing key); and

program means for:

determining by utilizing said public key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices (paragraphs 21-24, the CA is certifying that the key pair was generated within the device and issues a certificate);

Challener does not disclose an event auditing and reporting system. Felt discloses:

recording when a request for EK certificate fails (paragraphs 320-333);

tracking each failed request to identify TPM vendors with greater than a pre-established number of failures (the act of auditing is tracking each failed request with a pre-established number > 0); and

messaging said TPM vendors to update their security procedures (paragraphs 322, 323, 326, 327, 330, and 331, a message is generated and an event is posted).

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the system as disclosed by Challener with the system of auditing and reporting as disclosed by Felt in order to form a recorded history making it easier to track down intermittent problems [*Practical UNIX & Internet Security, Chapter 10, Auditing and Logging*].

Regarding claim 15:

Challener and Felt disclose the data processing system of claim 14, further comprising means for generating a certificate only when said public signing key matches a public signing key within said signing key certificate (paragraph 23 of Challener, there is a public key P2 (the endorsement key) is sent over along with the certificate C1 (of the signing key pair). The CA checks the accuracy of the certificate, C1, and then makes a certificate, C2, for public key, P2)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES TURCHEN whose telephone number is (571)270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571)272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139